REMARKS

The Office Action dated June 15, 2005 has been received and carefully noted. The following remarks are submitted as a full and complete response thereto. Claims 1-33 are currently pending in the application and are respectfully submitted for consideration.

As a preliminary matter, the Office Action alleges that the Applicants did not argue against the rejection of claims 26-30 in the previous Office Action, and therefore the Examiner has assumed that the Applicants agrees that the rejection of these claims were proper (Office Action, Page 3, lines 12-15). Applicants respectfully disagree and submit that the rejection of claims 25-33 was traversed in the Response filed on April 8, 2005. Specifically, on page 19 of the Response filed April 8, 2005, Applicants stated that "Davis does not disclose or suggest determining a second bit string corresponding to the random number, wherein the second bit string is received from the manufacturer of the electronic component," as recited in claim 25. In addition, Applicants submitted, on page 20 of the Response of April 8, 2005, that claims 26-33 are dependent upon claim 25 and therefore should be allowed for at least their dependence upon claim 25, and for the specific limitations recited therein. Consequently, Applicants have not conceded in any manner that the rejection of claims 25-33 is proper.

In the Office Action, claims 1-4, 6-16, and 18-24 were rejected under 35 U.S.C. §103(a) as being unpatentable over Tello (U.S. Patent No. 6,463,537) in view of Angelo (U.S. Patent No. 6,370,649). The Office Action took the position that Tello discloses all

of the elements of the claims, with the exception of a host configured to receive a guess passcode from a manufacturer. The Office Action then relies upon Angelo as allegedly curing this deficiency in Tello. The rejection is respectfully traversed for the reasons which follow.

Claim 1, upon which claims 2-14 are dependent, recites an apparatus for enabling functionality of a component. The apparatus includes a random number generating module for generating a random number, a hash function module in communication with the random number generating module, a host in communication with the random number generating module, at least one memory in communication with the host, an encryption module in communication with the memory, and a comparing device in communication with the encryption module and the hash function module. The comparing device compares a first bit string to a second bit string in order to generate a function enable output for the component. The host is configured to receive a guess passcode from the manufacturer of the component.

Claim 15, upon which claims 16-24 are dependent, recites a component for selectively enabling a functionality of an electronic device. The component includes a means for generating a random bit string, a hash function module in communication with the means for generating, a means for acquiring a guess passcode in communication with the means for generating, an encryption module in communication with the means for acquiring, and a comparing device in communication with the encryption module and the hash function module. The comparing device has an output for transmitting a

functionality enable signal therefrom. The means for acquiring the guess passcode is configured to acquire the guess passcode from the manufacturer of the electronic device.

The prior art has failed to produce enablement methods that are effective against reasonably sophisticated attackers. The claimed invention resolves the limitations of the prior art by providing, in one example, a cryptographic method wherein the secure portions of the method are implemented in electronic or computer products. More specifically, embodiments of the claimed invention implement cryptographic functions for enabling functionality of electronic/computer related components, wherein the relevant secure key related information is contained within computer hardware in a non-volatile memory device and not within a purely software driven configuration. The claimed invention also provides the ability to conduct secure functionality enablement on electronic/computer related components, wherein a public key for enabling the component is contained onboard and utilized in conjunction with a randomly generated component identifier in order to selectively enable additional functionality of the component.

As will be discussed below, Tello and Angelo, whether viewed singly or combined, fail to disclose or suggest the elements of the claims, and therefore fails to provide the advantages discussed above.

Tello discloses a modified computer motherboard security and identification system. More specifically, Tello discloses a modified motherboard with a microprocessor based security engine, enabling and disabling circuits, memory buffer

circuits, modified BIOS, modified DDL, and a smart card reader and smart cards. Upon startup of the computer, the modified BIOS takes control and allows the security engine microprocessor to look for and read from a smart card in the smart card reader that is connected to the security engine microprocessor. A unique hash number is placed in the smart card during the initial set up of the security system and a complimentary hash number is assigned to the security engine memory. During startup, a software program in the flash memory of the security engine compares the hash numbers in the smart card and the computer. If these two hash numbers are compliments, the boot up procedure is allowed to continue and access to the computer is allowed.

Angelo discloses a computer system with a self-modifying "fail-safe" password system that allows a manufacturer to securely supply a single-use password to users who lose or misplace a system password. The fail-safe password system utilizes a fail-safe counter, an encryption/decryption algorithm, a manufacturer's public key, and a secure non-volatile memory space. Each time a fail-safe password is entered into the computer system, an application decrypts the fail-safe password and compares the resulting value, which is a hash code, to an internal hash value and increments the fail-safe counter or modifies the seed value when the hashes match. When the fail-safe counter is incremented, the previous fail-safe password is no longer valid.

Applicants respectfully submit that the combination of Tello and Angelo fails to disclose or suggest all of the elements of claims 1 and 15. For example, Tello and Angelo do not disclose or suggest a hash function module in communication with a

random number generating module, as recited in present claims 1 and 15. The Office Action cites Tello as allegedly disclosing this limitation of the claims. However, Tello only discloses that an algorithm generates hash numbers H1, H2, H3 which are then encrypted to generate H1', H2', H3' (Tello, Column 8, lines 10-16). Tello does not disclose or suggest that the algorithm for generating the hash numbers is in communication with a random number generating module. In fact, nowhere does Tello explicitly disclose the use of a random number generating module. In addition, Angelo also does not disclose or suggest that a hash function module is in communication with a random number generating module. Therefore, Tello and Angelo, whether viewed individually or combined, fail to disclose or suggest at least this element of claims 1 and 15.

Applicants respectfully submit that Tello and Angelo also fail to disclose or suggest an encryption module in communication with at least one memory, as recited in claim 1. The Office Action specifically cites Column 24, lines 46-50 as allegedly disclosing this element of the claim. This section of Tello, however, merely discloses that an encrypted code number is read from an inserted smart card and decrypted using the public encryption key. Applicants respectfully assert that the smart card does not correspond to the memory of the present invention, and therefore Tello does not disclose that a memory is in communication with an encryption module. Applicants note that claim 1 recites that the memory is also in communication with the host. As such, the smart card of Tello does not correspond to the memory of the present invention.

Additionally, Angelo also does not disclose or suggest such a limitation. Therefore, Applicants respectfully submit that the combination of Tello and Angelo fails to disclose or suggest an encryption module in communication with at least one memory.

For at least the reasons discussed above, Applicants respectfully assert that claims 1 and 15 recite limitations that are neither disclosed nor suggested by the cited prior art. Thus, Applicants respectfully request that the rejection of claims 1 and 15 be withdrawn.

Applicants note that claims 2-14 and 16-24 are dependent upon claims 1 and 15, respectively. Consequently, claims 2-14 and 16-24 should be allowed for at least their dependence upon claims 1 and 15, and for the specific limitations recited therein.

Claims 5 and 17 were rejected under 35 U.S.C. §103(a) as being unpatentable over Tello in view of Angelo and further in view of Crouch (U.S. Patent No. 5,383,143). The Office Action took the position that Tello and Angelo disclose all of the elements of claims 5 and 17, with the exception of a linear feedback shift register, a NAND gate, and at least one inverter in communication with the linear feedback shift register and NAND gate. The Office Action then relies upon Crouch as allegedly curing these deficiencies in Tello and Angelo. The above rejection is respectfully traversed for the reasons which follow.

Tello and Angelo are discussed above. Crouch discloses a self re-seeding linear feedback shift register data processing system for generating a pseudo-random test bit stream. The data processing system 10 has a test controller 12 with a pattern generator 18 for receiving a seed value and generating many pseudo-random values from the seed

value. A re-seed and compare circuit 22 monitors the pattern generator 12 and determines when the seed value repeats in the pseudo-random number sequence generated by the generator 18. Once the compare circuit 22 determines that the seed value has repeated, the control circuit 20 allows the generator 18 to clock once more and latches a new seed value into the circuit 22.

Applicants note that claims 5 and 17 are dependent upon claims 1 and 15, respectively. Further, as discussed above, the combination of Tello and Angelo fails to disclose or suggest all of the elements of claims 1 and 15. Additionally, Crouch fails to cure those deficiencies in Tello and Angelo. As such, claims 5 and 17 should be allowed for at least their dependence upon claims 1 and 15, and for the specific limitations recited therein.

Claims 25-33 were rejected under 35 U.S.C. §103(a) as being unpatentable over Davis (U.S. Patent No. 5,577,121) in view of Tello and further in view of Angelo. The Office Action took the position that Davis discloses all of the elements of the claims, with the exception of the second bit string being encrypted using a public key and receiving the second bit string from a manufacturer of the electronic component. The Office Action then relies upon Tello and Angelo as allegedly curing this deficiency in Davis. The rejection is respectfully traversed for the reasons which follow.

Claim 25, upon which claims 26-33 are dependent, recites a method for enabling functionality of an electronic component. The method includes the steps of generating a random number, calculating a first bit string from the random number, determining a

second bit string corresponding to the random number, encrypting the second bit string with a public key to generate a third bit string, comparing the third bit string to the first bit string to determine a match, and outputting a function enable signal in accordance with the comparison. The step of determining the second bit string comprises receiving the second bit string from the manufacturer of the electronic component.

Tello and Angelo are discussed above. Davis discloses a transaction system for integrated circuit cards, and more specifically it discloses a method of conducting a transaction between an integrated circuit (IC) card and a transaction terminal which includes a security module. The method includes establishing communication between the terminal and the IC card and separately generating a session key in the IC card using data stored in the IC card and a code associated with the particular IC card and in the security module using data stored in the security module and the code associated with the particular IC card. The session key generated by the IC card is used to encrypt data using an encryption algorithm to obtain a first result and the session key generated by the security module is used to encrypt the same data using the same encryption algorithm to obtain a second result. The first and second results are compared and the terminal will conduct the transaction only if the comparison establishes that the first result and the second result are identical.

Applicants respectfully submit that the combination of Davis, Tello and Angelo fails to disclose or suggest all of the elements of claim 25. Specifically, Applicants respectfully submit that Davis, Tello, and Angelo all fail to disclose or suggest

determining a second bit string corresponding to the random number, as recited in claim 25. The Office Action cites Davis as allegedly disclosing this element of the claim. Applicants submit that Davis does not determine a second bit string which corresponds to the random number. Rather, according to Davis, the security module generates a random number and sends it to the SVC. The SVC encrypts the random number with the SVC session key. The security module encrypts the random number with the security module session key (Davis, Column 13, lines 6-52). Therefore, Davis only discloses generating a random number which is then encrypted by the SVC and security module. Davis does not disclose that a second bit string corresponding to the random number is determined. In addition, Tello and Angelo do not disclose or suggest such a limitation.

Furthermore, Davis does not disclose or suggest "encrypting the second bit string with a public key to generate a third bit string." Instead, Davis discloses encrypting the random number with the security module session key which is maintained exclusively within the memory of the security module (Davis, Column 13, lines 34-42). The Office Action alleges that it would have been obvious to a person of skill in the art to have used a public key as the type of encryption key is an arbitrary choice. Applicants respectfully disagree. Applicants respectfully submit that each type of encryption key has its advantages and drawbacks. In addition, certain encryption keys may not be appropriate for a certain applications. Therefore, Applicants respectfully submit that it would not have been obvious to a person of skill in the art to modify Davis, which uses a security module session key, to yield the claimed invention.

Additionally, Applicants respectfully submit that Davis fails to disclose or suggest outputting a function enable signal in accordance with the comparison between the third and first bit strings, as recited in claim 25. Davis merely discloses that "the result is compared with a derived password which the SVC retrieves from its memory. If the result is identical to the derived password stored in the SVC, the security module and correspondingly the POS terminal are verified and the establishment of a secure session is confirmed to the reader/writer" (Davis, Column 14, lines 1-7). Thus, Davis does not disclose or suggest a comparing device that outputs a function enable signal.

For at least the reasons discussed above, Applicants respectfully submit that the combination of Davis, Tello, and Angelo fails to disclose or suggest all of the elements of claim 25. As such, Applicants respectfully request that the rejection of claim 25 be withdrawn.

It is also respectfully submitted that claims 26-33 depend from claim 25 and therefore should be allowed for at least their dependence on claim 25, and for the specific limitations recited therein.

For the reasons stated above, Applicants respectfully submit that the cited prior art references fail to disclose or suggest critical and important elements of the claimed invention. These distinctions are more than sufficient to render the claimed invention unobvious. It is therefore requested that all of claims 1-33 be allowed, and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicant's undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

Majid S. AlBassam
Registration No. 54,749

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

MSA:jf